

## Claims

1. A digital data depository for storing digital data items for a user comprising:  
data storage means;  
a user account associated with the user; and  
means for establishing a digital data transaction session in which the user is able to instruct storage or retrieval of a digital data item in association with the user's account;  
means for encoding the data item into a plurality of parts, the parts being separately stored in the storage means; and  
means for decoding the encoded data item.
2. A depository as claimed in Claim 1 wherein the data storage means comprises at least one data storage device, the parts being separately stored on the data storage device or devices.
3. A depository as claimed in Claim 1 ~~or Claim 2~~ further comprising means for communication with the user.
4. A depository as claimed in ~~any one of the preceding claims~~<sup>1</sup> further comprising means for authentication of the user with the depository.
5. A depository as claimed in ~~any one of the preceding claims~~<sup>1</sup> further comprising means for authentication of the depository by the user.
6. A depository as claimed in ~~any one of the preceding Claims~~<sup>claim 1</sup> wherein the user is able to instruct retrieval of a copy of the item in said transaction session.
7. A depository as claimed in ~~any one of the preceding Claims~~<sup>claim 1</sup> wherein the user is able to instruct deletion of the digital data item in said transaction session.
8. A depository as claimed in ~~any one of the preceding Claims~~<sup>claim 1</sup> wherein the user is able to instruct an account status report in said transaction session.

09600297.071300  
00ET.0.26200960

9. A depository as claimed in <sup>claim 1</sup> ~~any one of the preceding Claims~~ wherein the user's account has a data structure identifying the user and containing information identifying the data items stored therein.

10. A depository as claimed in Claim 9 wherein the information of each data item includes at least one of the type, size, time/date of submission, period of storage and pointers to the locations of the stored parts of the data item.

11. A depository as claimed in <sup>claim 1</sup> ~~any one of the preceding Claims~~ wherein the means for encoding:

- a) divides the data item into a multiple of  $q$   $K$ -tuples, denoted as  $X_i = (x_{i1} \ x_{i2} \ \dots \ x_{iK})$ ,  $i = 1$  to  $q$ , where  $x_{ij}$  is a symbol over  $GF(2^m)$  with  $m$  being a positive integer;
- b) for  $i = 1$  to  $q$ , encodes  $X_i$  into a codeword  $Y_i = (y_{i1} \ y_{i2} \ \dots \ y_{iN})$  using an  $(N, K)$  error-control code  $C$ , where  $Y_{ij}$  is a symbol over  $GF(2^m)$ ;
- c) rearranges  $Y_i$ , for  $i = 1$  to  $q$ , into  $q$ -tuples  $Z_j = (y_{1j} \ y_{2j} \ \dots \ y_{qj})$ , for  $j = 1$  to  $N$ ; and
- d) stores the  $Z_j$ , for  $j = 1$  to  $N$ , as said parts.

12. A depository as claimed in claim 11 wherein the means for decoding :

- a) on inputting a data item identity, for  $j = 1$  to  $N$ , reads  $Z'_j = (y'_{1j} \ y'_{2j} \ \dots \ y'_{qj})$  from the locations where  $Z_j$  was stored, where  $Z_j$ ,  $j = 1$  to  $N$ , are the parts of the data item as identified
- b) rearranges  $Z'_j$ , for  $j = 1$  to  $N$ , into  $N$ -tuples  $Y'_i = (y'_{i1} \ y'_{i2} \ \dots \ y'_{iN})$ , for  $i = 1$  to  $q$ ;
- c) decodes  $Y'_i$  using an error-and-erasure-correction decoder of the  $(N, K)$  code  $C$  to obtain  $X'_i = (x'_{i1} \ x'_{i2} \ \dots \ x'_{iK})$ , for  $i = 1$  to  $q$ ; and
- d) concatenates  $X'_i$ , for  $i = 1$  to  $q$  to form the data item.

13. A depository as claimed in Claim 12 wherein the means for decoding:

- e) at step (a), if  $Z_j$  cannot be found, assigns  $Z'_j$  as a  $q$ -tuple of erasures, such that in  $Z'_j = (y'_{1j} \ y'_{2j} \ \dots \ y'_{qj})$  each symbol is marked as an erasure; otherwise leaving  $Z'_j$  unchanged;
- f) checks to see if all the decoding operations are successful and if not, raises an alarm.

00600297.071300

14. A depository as claimed in Claim 11 wherein the means for encoding computes an integrity check  $IC_j$  over  $Z_j$  for  $j=1$  to  $N$  and stores  $(Z_j, IC_j)$ , for  $j=1$  to  $N$ , as said parts.

15. A depository as claimed in Claim 14 wherein the means for decoding:

a) on inputting a data item identity, for  $j = 1$  to  $N$ , reads  $Z'_j = (Y'_{1j} Y'_{2j} \dots Y'_{qj})$  and  $IC'_j$  from the locations where  $(Z_j, C_j)$  was stored, where  $Z_j, j = 1$  to  $N$ , are the parts of the data item as identified and  $C_j$  are the parts of the corresponding integrity check

b) rearranged  $Z'_j$ , for  $j = 1$  to  $N$ , into  $N$ -tuples  $Y'_i = (y'_{i1} y'_{i2} \dots y'_{iN})$ , for  $i = 1$  to  $q$ ;

c) decodes  $Y'_i$  using an error-and-erasure-correction decoder of the  $(N, K)$  code  $C$  to obtain  $X'_i = (x'_{i1} x'_{i2} \dots x'_{iK})$ , for  $i = 1$  to  $q$ ; and

d) concatenates  $X'_i$ , for  $i = 1$  to  $q$  to form the data item.

16. A depository as claimed in Claim 15 wherein the means for decoding:

e) at step (a), if  $Z_j$  cannot be found, assigns  $Z'_j$  as a  $q$ -tuple of erasures, such that in  $Z'_j = (y'_{1j} y'_{2j} \dots y'_{qj})$  each symbol is marked as an erasure; otherwise verifying the integrity of  $Z'_j$  based on  $IC'_j$ , if  $Z'_j$  fails the integrity verification, marking it as a  $q$ -tuple of erasures; otherwise leaving  $Z'_j$  unchanged;

f) checks to see if all the decoding operations are successful and if not, raises an alarm.

17. A depository as claimed in ~~any one of the preceding claims~~<sup>1</sup> further comprising means for encryption of the data item.

18. A depository as claimed Claim 17 wherein the user is able to instruct encryption, prior to encoding, of the data item to be stored during the transaction session.

19. A depository as claimed Claim 18 as dependent directly or indirectly on Claim 9 wherein the information of each data item includes an indication of whether or not the item is encrypted and a pointer to a decryption key.

20. A depository as claimed in <sup>claim 1</sup> ~~any one of the preceding Claims~~ further comprising means for decryption of an encrypted data item.

09600297.021300

21. A depository as claimed in <sup>claim 1</sup>~~any one of the preceding Claims~~ further comprising means for checking the encoded data items.
22. A depository as claimed in Claim 21 wherein the means for checking decodes, checks and reencodes the data item at intervals.
23. A depository as claimed in Claim 22 wherein the intervals are of fixed or variable period.
24. A depository as claimed in <sup>claim 1</sup>~~any one of the preceding Claims~~ further comprising means for verifying the integrity of the data item and the data item includes an integrity check to be verified.
25. A depository as claimed in Claim 24 wherein the integrity check comprises a digital signature.
26. A depository as claimed in Claim 24 wherein the integrity check comprises a message authentication code.
27. A depository as claimed in <sup>claim 1</sup>~~any one of the preceding Claims~~ wherein communication with the user during the transaction session is by means of a plurality of messages each associated with a transaction to be performed.
28. A depository as claimed in Claim 27 wherein at least one of said messages contains a freshness identifier.
29. A depository as claimed in Claim 28 wherein the freshness identifier comprises a timestamp, sequence number or a nonce.
30. A method of operating a depository as claimed in <sup>claim 1</sup>~~any one of the preceding Claims~~.

31. A method of storing digital data items for a user comprising the steps of:  
providing a user account associated with the user;  
authenticating the identity of the user;  
receiving a digital data item and an instruction from the user for the item to be stored in  
association with the user's account; and  
encoding the data item into a plurality of parts and storing the parts separately.

32. A method as claimed in Claim 31 further comprising the steps of:  
receiving an instruction to retrieve a stored and encoded data item, decoding the data item  
and sending the data item to the user.

33. A method of protecting digital data comprising:  
providing a data depository in which digital data may be stored electronically;  
providing for registration of users of the data depository, each user having an  
account with the depository;

in response to a request from a user, opening a transaction session with the user in  
which the user and the depository authenticate each other and performing a transaction  
instructed by the user in respect of a digital data item, the transaction being selected by the  
user from a plurality of available transactions including storage of the item in or retrieval  
of the item from the depository.

34. A method as claimed in Claim 33 in which storage of the item includes encoding  
the item into a plurality of parts and storing the parts separately in the depository.

35. A method as claimed in claim 33 or ~~Claim 34~~ further comprising the step of  
checking, at intervals, the integrity of data items stored in the depository.

09600297.07.1300  
00ET/0" 26200960